

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

| | | |
|--------------------------------------|---|-------------------------|
| NICHOLAS MARTIN on behalf of himself |) | |
| and others similarly situated, |) | |
| |) | |
| Plaintiff, |) | Case 1:10-cv-3494 |
| |) | |
| v. |) | Judge Dow |
| |) | |
| CCH, INCORPORATED, |) | Magistrate Judge Ashman |
| |) | |
| Defendant. |) | |

**DEFENDANT’S REPLY IN SUPPORT OF MOTION TO
DISMISS COUNT I OF PLAINTIFF’S AMENDED COMPLAINT**

Defendant CCH, Incorporated, by and through its counsel, and pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, respectfully submits this Reply in Support of its Motion to Dismiss Count I of Plaintiff Nicholas Martin’s (“Martin”) Amended Complaint.

INTRODUCTION

In order to avoid the preemptive effect of the CAN-SPAM Act, Plaintiff must show that the subject lines of the emails he received are deceptive or misleading. Notwithstanding this necessity, Plaintiff acknowledges that there is nothing deceptive or misleading about the email subject lines. Pls’ Br. 17 (“they accurately tell the recipient that there is an advertisement inside”); Pls’ Br. at 1 (“the email subject lines seem harmless enough on their face”). Instead, Plaintiff claims that they “surreptitiously monitor plaintiff’s actions and location.” However, what Plaintiff complains of is no different than certified mail or an email sender requesting a read receipt for an email, which is even part of the routine practice for counsel for the Plaintiff. The complained of activity is sufficiently common-place that it is inherently free of deception or the ability to mislead. Consequently, Plaintiff’s claim under the Illinois Electronic Mail Act, 815

ILCS § 511/1 *et seq.* (“IEMA”), is expressly preempted by the Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C.A. §§ 7701 *et seq.* (“CAN-SPAM Act”).

FACTS

Two emails comprise the factual context for Plaintiff’s complaint. The subject line of the first email states “Buy now pay Feb. 15.” This email goes on to offer exactly that which was advertised—tax software with a deferred payment due on February 15, 2010. The second email’s subject line similarly states “Offer extended – Buy now pay Feb. 15.” This email again offers Plaintiff the opportunity to purchase tax software with a deferred payment until February 15, 2010.

Plaintiff claims that these email subject lines are misleading and deceptive because “[h]idden within each of these emails is sophisticated computer code that allows CCH to gather private information about the recipients whereabouts and actions.” Pl’s Br. 1. At bottom, Plaintiff confuses two different things: (1) when an email is sent, if allowed, the images contained in the email can download on the computer, which can then provide the sender with two innocuous pieces of information: the recipient’s IP address and the date/time that the recipient accessed the email¹ and (2) when a individual accesses a website, a cookie can be downloaded on the recipient’s computer, which can track access and use of a website.

Plaintiff cites lengthy passages from the FTC and from a CCH privacy policy, but these all involve privacy concerns related to accessing *websites*. Pl’s. Br. 4 (“Online behavioral advertising involves the tracking of consumers’ online activities . . .”); Pl’s. Br. 4 (as an example of behavioral advertising “a consumer visits a travel website...”); Pl’s Br. 4 (a consumer’s access to a travel website combined with a consumer’s access to a newspaper’s website can be tailored);

¹ However, most email providers, including Plaintiff’s Hotmail, have functions that restrict this access unless the email opener, in addition to opening the email, separately agrees to view the images contained within the email.

Pl's Br. 15 ("Every website where data is collected..."). Further, cookies are downloaded on a computer when a *website* is accessed. Pl's Br. 5; Ex. C, p. 2 ("A cookie is a small text file that is placed on a user's hard drive *by a web browser* at the request *of a web page server*. Cookies cannot be used to run programs, deliver viruses to your computer, or extract personal information from your computer. . . Cookies may also enable us to track and target the interests of our users in order to enhance the experience customers have *while on our sites.*") (emphasis added). Although Plaintiff persistently references websites, in the present matter, there are no allegations that Plaintiff visited Defendant's website—the only issue relates to the emails themselves.

Plaintiff also inaccurately claims that the images in the emails are downloaded "automatically" to Plaintiff's computer, which then transmits an IP address and date/time of access. However, most email providers, including Plaintiff's Hotmail, have functions that restrict this access, requiring individuals to authorize such downloads. This was undoubtedly an option for Plaintiff.

Insofar that Plaintiff asserts that Defendant engaged in "online behavioral advertising," "profiling," tracking online activities, placing cookies on his computer, and monitoring access to its website, this is unsupported by the allegations in this case. These arguments, and therefore much of Plaintiff's brief, must be disregarded as irrelevant. At issue are only the subject lines of the emails themselves. Thus, Plaintiff claims that they are misleading or deceptive because they fail to inform him that accessing the email allegedly could reveal two pieces of information: (1) the recipient's IP address and (2) the date/time the email was accessed. Such innocent information is not deceptive or misleading.

ARGUMENT

I. The subject lines of the emails sent to Plaintiff are not false or misleading.

Plaintiff and Defendant agree on the basic law: the CAN-SPAM Act pre-empts the IEMA unless the subject lines of the emails are deceptive or misleading. As both the Fourth and Ninth Circuits have concluded, this narrow exception only applies to traditionally tortious or wrongful conduct. *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 359 (4th Cir. 2006) (the coupling of “falsity” with “deception” indicated Congress intended “falsity” to equate with torts involving misrepresentations); *Gordon v. Virtumundo*, 575 F.3d 1040, 1062 (9th Cir. 2009) (“we are likewise persuaded that the exception language, read as Congress intended, refers to ‘traditionally tortious or wrongful conduct.’”). Where the parties disagree is whether the subject lines of the emails are false or misleading.

Plaintiff must establish that (1) CCH made a false statement of material fact; (2) CCH knew or believed that the statements were false, or the statements were made with a reckless disregard of whether they were true or false; (3) the statements were made with the intent to induce action; (4) Martin reasonably believed the statements and justifiably acted in reliance on those statements; and (5) Martin suffered damages as a result. *Extra Equipamentos E Exportacao Ltda. v. Case Corp.*, 541 F.3d 719, 732 n.4 (7th Cir. 2008) (applying Illinois law). Specifically, Plaintiff claims that by accessing the emails, the following information is revealed (1) recipient’s IP address; and (2) date/time that the recipient accessed the email. However, Plaintiff’s claim that the e-mails may gather data regarding the recipient has nothing to do with any fraudulent conduct.²

² To the extent that Plaintiff, now, for the first time, claims that the emails are deceptive or misleading, Plaintiff must comply with Rule 9(b) pleading requirements, which he has not. Fed. R. Civ. P. 9(b) (“[i]n all averments of fraud ..., the circumstances constituting fraud ... shall be stated with particularity”); *see*

In the present matter, Plaintiff is incapable of meeting the above burden. The Ninth Circuit has found that where the email headers at issue are not aimed at misleading recipients, there is no fraud. *See Gordon v. Virtumundo*, 575 F.3d at 1064. (offers no proof that any headers have been altered to impair a recipient's ability to identify, locate, or respond to the person who initiated the email. Nor does he present evidence that [defendant's] practice is aimed at misleading recipients . . ."). Only traditional fraud and deception are exempted from the preemption of the CAN-SPAM Act. *See Kleffman v. Vonage Holdings Corp.*, No. 07-2406, 2007 U.S. Dist. LEXIS 40487, at *4-5 (C.D. Cal. May 22, 2007) ("while he might characterize an email as containing the implicit misrepresentation . . . , this is more than the plain language of the statute would bear. And even if the statute did create such an innovative cause of action, it would be preempted because, the Court concludes, the CAN-SPAM Act left states room only to extend *traditional* fraud and deception prohibitions into cyberspace.") (emphasis added). Further, Plaintiff has in no way shown any damages, which is required for the traditional tort of misrepresentation.

These holdings are perfectly consistent with logic and other means of providing similar advertising. Were the Defendant to have used certified mail to send an identical message, Defendant would have received the exact same information, or more than that received through the email which need not be opened. Unlike certified mail, where the recipient is sought out and delivered the message, emails need not be opened. In addition to gathering the same information as that complained of here, certified mail deliverers can indicate whether a particular recipient resisted or refused to accept the material. At its core, Plaintiff is complaining of a widely used

also DiLeo v. Ernst & Young, 901 F.2d 624, 627 (7th Cir. 1990) (describing Rule 9(b) particularity as "the who, what, when, where, and how: the first paragraph of any newspaper story").

practice that is more innocuous than certified mail and can be altogether avoided by just deleting the email or declining to view the images.

Notably, Plaintiff has failed to allege that either the substance of the message or its header were misleading or violative of a traditional tort theory. Absent even this, Plaintiff's attempt to recover for actions that are less intrusive than certified mail cannot be credited.

II. Plaintiff's claims are preempted by the CAN-SPAM Act.

Because there is nothing misleading or deceptive about the subject lines of the emails, Plaintiff's claim is preempted by the CAN-SPAM Act. 15 U.S.C. § 7707(b)(1) ("This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.") Congress's clearly expressed purpose in enacting the CAN-SPAM Act preempts the application and enforcement of IEMA in this case. *See Kleffman v. Vonage Holdings Corp.*, 2007 U.S. Dist. LEXIS 40487, at *9-10 (dismissing claim finding that state statute regulating e-mail was preempted by CAN-SPAM Act).

CONCLUSION

For all of the reasons set forth in Defendant's Motion to Dismiss, Memorandum in Support of its Motion to Dismiss, and above, Nicholas Martin's Illinois Electronic Mail Act claim is preempted by federal law. Defendant's Motion to Dismiss Count I of the Amended Complaint should be granted, with prejudice.

DATED: September 24, 2010

Respectfully submitted,

By: /s/ David L. Hartsell

David L. Hartsell
Susan E. Groh
McGUIREWOODS LLP
77 W. Wacker Drive, Ste. 4100
Chicago, IL 60601
(312) 849-8100
dhartsell@mcguirewoods.com
sgroh@mcguirewoods.com

CERTIFICATE OF SERVICE

I hereby certify that on September 24, 2010, I electronically filed the foregoing **DEFENDANT'S REPLY IN SUPPORT OF MOTION TO DISMISS COUNT I OF PLAINTIFF'S AMENDED COMPLAINT** with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following:

Alexander H. Burke
BURKE LAW OFFICES, LLC
155 N. Michigan Ave., Suite 9020
Chicago, IL 60601
ABurke@BurkeLawLLC.com

/s/ David L. Hartsell
